REMARKS

Claims 1-47, 49 and 50 are all the claims pending in the application.

I. Objections to the Specification

In item 1 of the Office Action, the Examiner objected to the specification because hyperlinks were included on pages 11 and 172 of the specification. Initially, it is noted that while hyperlinks are included on pages 10 and 171 of the specification, it does not appear as though pages 11 and 172 include hyperlinks. In this regard, Applicants note that the hyperlinks on pages 10 and 171 of the specification have been removed by this amendment. Accordingly, Applicants kindly request that the objections be reconsidered and withdrawn.

II. Objection to the Claims

In item 2 of the Office Action, the Examiner has objected to claim 26 due to a minor informality. Regarding this objection, Applicants note that the Examiner made the identical objection in the previous Office Action, and that in response thereto, Applicants amended claim 26 in the amendment filed on April 19, 2007 in order to correct this typographical error. In particular, it is noted that the term "confirm" in claim 26 was changed to --conform--. Accordingly, Applicants kindly request that the objection be reconsidered and withdrawn.

III. Double Patenting

In item 2 of the Office Action, the Examiner has rejected claims 1-12, 14-32 and 36-51 because the Examiner believes that such claims conflict with claims 1-7, 9-33, 37-40 and 43 of

copending Application No. 10/725,208 (hereafter "the '208 application"). As such, the Examiner has taken the position that Applicants are required to cancel the conflicting claims from all but one application (see Office Action at page 2). Applicants respectfully disagree with Examiner's position.

In particular, Applicants note that MPEP § 822, which is the section of the MPEP relied on by the Examiner, indicates that the requirement to cancel conflicting claims in copending applications should "be used when the conflicting claims are identical or conceded by applicant to be not patentably distinct" (emphasis added). In this regard, Applicants note that the claims identified by the Examiner in the present application and in the '208 application are not identical and, further, Applicants submit that such claims are patentably distinct.

If the Examiner believes that the claims of the present application are patentably indistinct from the claims of the '208 application, then the Examiner should make an obviousness type double patenting rejection, and must explain why the claims of the present application are considered obvious in view of the claims of the '208 application. The Examiner has not performed this analysis. Instead, the Examiner has merely pointed to several features in the claims of the present application and the '208 application and has indicated that such features are "equivalent" or that such features "may be the same". This is not a proper analysis for an obviousness-type double patenting rejection, and therefore, the Examiner's double patenting rejection is traversed.

To the extent that the Examiner makes an obviousness-type double patenting rejection of the claims of the present application based on the claims of the '208 application, Applicants submit the following arguments.

Regarding claim 1, Applicants note that claim 1 of the present application recites the feature of a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted, whereas claim 1 of the '208 application recites the feature of a judging unit operable to judge, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted.

Applicants respectfully submit that it would not have been obvious, based on claim 1 of the '208 application to provide a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted.

Regarding the above-noted features, the Examiner has indicated in the Office Action that "re-encryption information may be the same as the verification values" (see Office Action at page 42). Initially, Applicants respectfully submit that the statement "may be the same as" has no bearing whatsoever on an obviousness determination. In addition, Applicants point out to the Examiner that in claim 1 of the present application, the "first decryption verification value" is generated by the "first decryption unit", and the "second decryption verification value" is generated by the "second shared-key generating unit". Thus, the two pieces of

information that are utilized by the "judging unit" are generated by the "first decryption unit" and the "second shared-key generating unit".

In contrast, in claim 1 of the '208 application, the "encryption information" is generated by the "encryption unit", and the "re-encryption information" is generate by the "re-encryption unit". As such, in claim 1 of the '208 application, the two pieces of information that are utilized by the "judging unit" are generated by the "encryption unit" and the "re-encryption unit".

In view of at least the foregoing, Applicants respectfully submit that claim 1 of the present application and claim 1 of the '208 application are clearly patentably distinct from one another. As noted above, if the Examiner disagrees, then the Examiner must explain why the features of claim 1 of the present application would be considered obvious in view of claim 1 of the '208 application.

In addition, regarding claim 1 of the present application and claim 1 of the '208 application, Applicants note that claim 1 of the present application recites the features of a first encryption unit operable to encrypt the verification value to generate first encryption information, and a second encryption unit operable to encrypt the seed value based on the verification value to generate second encryption information, whereas claim 1 of the '208 application recites the feature of an encryption unit operable to encrypt the seed value based on the blind value to generate encryption information.

Applicants respectfully submit that it would not have been obvious, based on claim 1 of the '208 application, which merely recites the feature of an encryption unit operable to encrypt

the seed value based on the blind value to generate encryption information, to provide a first encryption unit operable to encrypt the verification value to generate first encryption information, and a second encryption unit operable to encrypt the seed value based on the verification value to generate second encryption information, as recited in claim 1 of the present application.

Further, Applicants note that claim 1 of the present application also recites the features of a first decryption unit operable to decrypt the first encryption information to generate a first decryption verification value, and a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value to generate a decryption seed value, whereas claim 1 of the '208 application recites the feature of a decryption unit operable to decrypt the encryption information to generate a decryption seed value.

Applicants respectfully submit that it would not have been obvious, based on claim 1 of the '208 application, which merely recites the feature of a decryption unit operable to decrypt the encryption information to generate a decryption seed value, to provide a first decryption unit operable to decrypt the first encryption information to generate a first decryption verification value, and a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value to generate a decryption seed value, as recited in claim 1 of the present application.

Moreover, Applicants note that claim 1 has been amended herein so to recite that the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses, and that the first encryption information and the second encryption information are

separate pieces of information. Applicants respectfully submit that such features would not have been obvious in view of the claims of the '208 application.

Regarding independent claim 3 of the present application and independent claim 3 of the '208 application, Applicants note that claim 3 of the present application recites the features of a first encryption unit operable to encrypt the verification value to generate first encryption information, and a second encryption unit operable to encrypt the seed value based on the verification value to generate second encryption information, wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses, and the first encryption information and the second encryption information are separate pieces of information. In contrast, claim 3 of the '208 application merely recites the feature of an encryption unit operable to encrypt the seed value based on the blind value to generate encryption information.

For at least similar reasons as discussed above with respect to claim 1 of the present application, Applicants respectfully submit that it would not have been obvious to provide the above-noted features recited in claim 3 of the present application based on the claims of the '208 application.

Regarding independent claim 24 of the present application and independent claim 21 of the '208 application, Applicants note that claim 24 of the present application recites the features of a first decryption unit operable to decrypt the first encryption information to generate a first decryption verification value; a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value to generate a decryption

seed value; and a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted, wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses, and the first encryption information and the second encryption information are separate pieces of information. In contrast, claim 21 of the '208 application merely recites the features of a decryption unit operable to decrypt the encryption information to generate a decryption seed value; and a judging unit operable to judge, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted.

For at least similar reasons as discussed above with respect to claim 1 of the present application, Applicants respectfully submit that it would not have been obvious to provide the above-noted features recited in claim 24 of the present application based on the claims of the '208 application.

Regarding independent claims 46 and 47 of the present application and independent claim 38 and 39 of the '208 application, Applicants note that claims 46 and 47 of the present application recite the features of a first encryption step of encrypting the verification value to generate first encryption information, and a second encryption step of encrypting the seed value based on the verification value to generate second encryption information, wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses, and the first encryption information and the second encryption information are separate pieces of information. In contrast, claims 38 and 39 of the '208 application merely recite the feature of

an encryption step of encrypting the seed value based on the blind value to generate encryption information.

For at least similar reasons as discussed above with respect to claim 1 of the present application, Applicants respectfully submit that it would not have been obvious to provide the above-noted features recited in claims 46 and 47 of the present application based on the claims of the '208 application.

Regarding independent claims 49 and 50 of the present application and independent claims 41 and 42 of the '208 application, Applicants note that claim 49 and 50 of the present application recite the features of a first decrypting step of decrypting the first encryption information to generate a first decryption verification value; a second decryption step of decrypting the second encryption information based on the first decryption verification value to generate a decryption seed value; and a judging step of judging, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted, wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses, and the first encryption information and the second encryption information are separate pieces of information. In contrast, claims 41 and 42 of the '208 application merely recite the features of a decryption step of decrypting the encryption information to generate a decryption seed value; and a judging step of judging based, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted.

For at least similar reasons as discussed above with respect to claim 1 of the present application, Applicants respectfully submit that it would not have been obvious to provide the above-noted features recited in claims 49 and 50 of the present application based on the claims of the '208 application.

Regarding dependent claims 2, 4-12, 14-23, 25-32 and 36-45 of the present application, Applicants submit that these claims are patentably distinct from the claims in the '208 application for at least the same reasons as discussed above regarding independent claims 1, 3, 24, 46, 47, 49 and 50.

IV. Claim Rejections under 35 U.S.C. § 102

The Examiner has rejected claims 1-15, 18-29, 32-46, 47, 49 and 50 under 35 U.S.C. § 102(b) as being anticipated by Hoffstein (WO/9808323).

Claim 1, as amended, recites the features of a first shared-key generating unit operable to generate a verification value and a shared key from the seed value; a first encryption unit operable to encrypt the verification value to generate first encryption information; a second encryption unit operable to encrypt the seed value based on the verification value, to generate second encryption information; a first decryption unit operable to decrypt first encryption information, to generate a first decryption verification value; a second decryption unit operable to decrypt second encryption information based on the first decryption verification value, to generate a decryption seed value; a second shared-key generating unit operable to generate a second decryption verification value and a decryption shared key, from the decryption seed

value; and a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted, wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses, and the first encryption information and the second encryption information are separate pieces of information. Applicants respectfully submit that Hoffstein does not disclose or suggest such a combination of features.

For the Examiner's reference, Applicants are including herein the following description of Hoffstein, which has been reproduced from the previous response filed on April 19, 2007.

In particular, Applicants note that Hoffstein discloses an encoding technique in which a secret key and a public key are generated by a first user (e.g., Dan) (see page 15, lines 23-25 and page 16, lines 7-12). As explained in Hoffstein, if a second user (e.g., Cathy) wants to send a message to Dan using his public key, she chooses a polynomial at random, and uses this polynomial, along with Dan's public key and her plaintext message, to create an encoded message to send to Dan (see page 16, lines 14-26).

In this regard, Applicants note that Fig. 2 of Hoffstein depicts the above-noted technique, in which the procedure begins at step 210 with Dan generating a public key and a private key, and then publishing the public key (i.e., sending the public key to Cathy) (see page 22, lines 3-23). Next, in step 240, Cathy encodes a plaintext message using the public key generated by Dan, and the encrypted message is transmitted (see Fig. 2 and page 22, line 24 through page 23, line 4). Upon receipt of the encrypted message, Dan then decodes the encrypted message using his generated private key (see Fig. 2 and page 23, lines 5-11).

Thus, in Hoffstein, Dan first generates a public key and a private key, and then sends the public key to Cathy, whereby Cathy uses the public key generated by Dan to encrypt a message that is transmitted to Dan, and upon receipt of the encrypted message, Dan uses his private key to decrypt the encrypted message.

With respect to the above-noted features recited in claim 1, Applicants note that in the response filed on April 19, 2007, Applicants took the position that Hoffstein does not disclose or suggest such features, and provided a detailed explanation as to why Hoffstein cannot be interpreted as disclosing such features.

In response to this argument, the Examiner has indicated the following in the present Office Action: (1) that the first shared-key generating unit and the second-shared key generating unit may be the same unit (i.e., Dan); (2) that "verification values" correspond to the results of the calculations for encryption/decryption and generation of a shared-key that are performed by Dan; (3) that the "decryption seed value" is generated by Dan because the "seed values" which are inserted into the polynomial formulas must be correct in order for decryption to succeed; and (4) that the "decryption seed values" would be the successful result of the polynomial calculations (see Office Action at pages 43-44).

Initially, regarding the Examiner's position that the first shared-key generating unit and the second shared-key generating unit may be the same unit, while Applicants disagree with this position, in order to clarify the meaning of claim 1, it is noted that claim 1 has been amended herein to recite that the shared-key generation apparatus (which includes the first shared-key generating unit) and the shared-key recovery apparatus (which includes the second shared-key

generating unit) are separate apparatuses. Accordingly, Applicants respectfully submit that the Examiner's above-noted position with respect to the first and second shared key generating units being the same unit no longer applies to amended claim 1.

In addition, with respect to the Examiner's position that certain values and results of the formulas in Hoffstein somehow correspond to the features of claim 1, Applicants respectfully submit that this is merely a blanket statement that has been made on the part of the Examiner, without taking into account the relationships between the features recited in claim 1.

For example, with respect to the Examiner's position that the "seed values" are inserted into the polynomial formulas in Hoffstein, and that the "verification values" correspond to the results of the calculations for encryption/decryption and generation of a shared key that are performed by Dan, Applicants note the following.

First, with respect to the "seed value", Applicants note that claim 1 recites the feature of a seed value generating unit that is operable to generate the seed value. The Examiner has not pointed to any features in Hoffstein which allegedly correspond to the "seed value generating unit", but instead, has merely indicated that "seed values" are inserted into the polynomial formulas.

Second, as noted above, claim 1 recites (1) that a first shared-key generating unit is operable to generate the verification value from the seed value, (2) that a first encryption unit is operable to encrypt the verification value, (3) that a second encryption unit is operable to encrypt the seed value based on the verification value, (4) that a first decryption unit is operable to decrypt first encryption information to generate a first decryption verification value, (5) that a

second decryption unit is operable to decrypt second encryption information based on the first decryption verification value to generate a decryption seed value, and (6) that a second shared-key generating unit is operable to generate a second decryption verification value, from the decryption seed value.

Regarding the above-noted features, initially, Applicants note that the Examiner has not pointed to any elements in Hoffstein which allegedly correspond to the above-noted features, but instead, as noted above, has merely made a blanket statement that the "seed values" are inserted into the polynomial formulas in Hoffstein, and that the "verification values" correspond to the results of the calculations for encryption/decryption and generation of a shared key that are performed by Dan.

Further, as is clear from the above-noted features (1) through (7), there are particular relationships between the various features, which Applicants submit that the Examiner has not addressed in the Office Action. As one example, in features (1) and (3), it is indicated that the first shared-key generating unit generates the verification value from the seed value, and that the second encryption unit encrypts the seed value based on the verification value. Using the Examiner's position that "the seed values" are inserted into the polynomial formulas, and that the "verification values" correspond to the results of the calculations, it is clear that the Examiner's position could not result in both of the above-noted features (1) and (3).

As another example, in feature (5) above, it is indicated that the second decryption unit is operable to decrypt second encryption information based on the first decryption verification value to generate a decryption seed value. As noted above, the Examiner has taken the position

that both of the first decryption verification value and the decryption seed value are the results of calculations in Hoffstein. It is clear, however, that if the Examiner is taking the position that both of these features correspond to the results of certain formulas in Hoffstein, that such a position is not consistent with the above-noted feature (5) which involves the decryption seed value being generated based on the first decryption verification value.

As yet another example, in feature (6) above, it is indicated that the second shared-key generating unit is operable to generate a second decryption verification value, from the decryption seed value. Again, using the Examiner's position that both of the second decryption verification value and the decryption seed value are the results of calculations in Hoffstein, it is clear that such a position is not consistent with the above-noted feature (6) which involves the generation of the second decryption verification value from the decryption seed value.

In view of the foregoing, Applicants submit that Hoffstein does not disclose, suggest or otherwise render obvious at least the above-noted combination of features recited in claim 1. Accordingly, Applicants submit that claim 1 is patentable over Hoffstein, an indication of which is kindly requested.

If the Examiner maintains the rejection of claim 1, Applicants request that the Examiner explicitly identify the particular elements of Hoffstein that allegedly correspond to each of the features recited in claim 1 so that Applicants may make an informed decision with regard to appeal. For example, if the Examiner is taking the position that a value of claim 1 corresponds to one of the values in the equations of Hoffstein, Applicants request that the Examiner explicitly identify the equation and particular value in that equation which are being relied

upon, and similarly, if the Examiner relies on results of certain equations in Hoffstein as allegedly corresponding to features of claim 1, Applicants request that the Examiner explicitly identify the particular equation and result that is being relied upon.

Regarding claim 2, Applicants note that this claim depends from claim 1 and is therefore considered patentable at least by virtue of its dependency.

Regarding claim 3, Applicants note that this claim recites the feature of a seed value-generating unit operable to generate a seed value; a shared-key generating unit operable to generate a verification value and a shared key, from the seed value; and a second encryption unit operable to encrypt the seed value based on the verification value, to generate second encryption information, wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses, and the first encryption information and the second encryption information are separate pieces of information.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious such a combination of features. Accordingly, Applicants submit that claim 3 is patentable over Hoffstein, an indication of which is kindly requested. Claim 4-15 and 18-23 depend from claim 3 and are therefore considered patentable at least by virtue of their dependency.

Regarding claim 24, Applicants note that this claim is drawn to a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus, the shared-key generation apparatus generating a seed value, generating a shared key from the seed value, and encrypting the seed value to generate second encryption information, wherein the shared-key

recovery apparatus includes a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value; a shared-key generating unit operable to generate a second decryption verification value and a decryption shared key, from the decryption seed value and according to a same method as used in the shared-key generation apparatus; and a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted, wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses, and the first encryption information and the second encryption information are separate pieces of information.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious such a combination of features. Accordingly, Applicants submit that claim 24 is patentable over Hoffstein, an indication of which is kindly requested.

Regarding claims 25-29 and 32-45, Applicants note that these claims depend from claim 24 and are therefore considered patentable at least by virtue of their dependency.

Regarding claims 46 and 47, Applicants note that each of these claims recites the features of a seed-value generating step of generating a seed value; a shared-key generating step of generating a verification value and shared key, from the seed value; and a second encryption step of encrypting the seed value based on the verification value, to generate second encryption information, wherein the shared-key generation apparatus and the shared-key recovery

apparatus are separate apparatuses, and the first encryption information and the second encryption information are separate pieces of information.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious such a combination of features. Accordingly, Applicants submit that claims 46 and 47 are patentable over Hoffstein, an indication of which is kindly requested.

Regarding claims 49 and 50, Applicants note that these claims are drawn to a shared-key recovery method and program used in a shared-key recovery apparatus that receives a shared key from a shared-key generating apparatus, the shared-key generation apparatus generating a seed value, generating a shared key from the seed value, and encrypting the seed value to generate second encryption information, wherein the shared-key recovery method includes a second decryption step of decrypting the second encryption information based on the first decryption verification value, to generate a decryption seed value; a shared-key generating step of generating a second decryption verification value and a decryption shared key, from the decryption seed value and according to a same method as used in the shared-key generation apparatus; and a judging step of judging, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted, wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses, and the first encryption information and the second encryption information are separate pieces of information.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious such a combination of features. Accordingly, Applicants submit that claims 48 and 49 are patentable over Hoffstein, an indication of which is kindly requested.

V. Claim Rejections under 35 U.S.C. § 103(a)

The Examiner has rejected claims 16, 17, 30, 31, 48 and 51 under 35 U.S.C. § 103(a) as being unpatentable over Hoffstein (WO/9808323).

Claims 16 and 17 depend from claim 3; and claims 30 and 31 depend from claim 24. As discussed above, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious all of the features recited in claims 3 and 24. Accordingly, Applicants submit that claims 16, 17, 30 and 31 are patentable at least by virtue of their dependency.

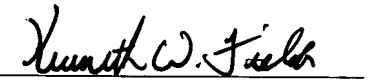
VI. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited.

If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Masato YAMAMICHI et al.

By: 

Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/ra
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
November 16, 2007